

AMENDMENT AND PRESENTATION OF CLAIMS

Please replace all prior claims in the present application with the following claims, in which claims 36-38 are newly presented.

1. (Previously Amended) A method for performing redundancy switching from a first platform to a second platform, the method comprising:

identifying a message received over an unspoofed connection according to a prescribed protocol as an unspoofed message;

tearing down, during a predetermined period, the unspoofed connection based upon the identifying step; and

restarting a spoofed connection between the second platform and a host, wherein the second platform serves as a redundant platform for the first platform, and the predetermined period is set to minimize delay for restarting of the spoofed connection.

2. (Previously Amended) The method according to claim 1, further comprising:

invoking a reset function, wherein the reset function transmits a reset message to a local host that forwarded the message to tear down the unspoofed connection.

3. (Original) The method according to claim 1, further comprising:

determining whether the predetermined period has expired; and

forwarding unspoofed messages to a remote platform based upon the determining step.

4. (Original) The method according to claim 1, wherein the prescribed protocol is the Transmission Control Protocol, the method further comprising:

determining whether global TCP spoofing is enabled; and

selectively forward TCP segments unspoofed to a remote platform.

5. (Original) The method according to claim 1, further comprising:

establishing a backbone connection from the second platform to a remote platform; and

forwarding a spoofed message over the backbone connection to a remote host.

6. (Original) The method according to claim 5, wherein the backbone connection in the establishing step includes a space link over a satellite network.

7. (Original) The method according to claim 1, further comprising:

forwarding messages associated with another protocol to a remote platform irrespective of the predetermined period.

8. (Previously Amended) A communication system comprising:

a first platform configured to communicate with a remote platform; and

a second platform configured to communicate with the remote platform upon failure of the first platform to communicate with the remote platform, the second platform being configured to identify a message received from a local host over unspoofed connection according to a prescribed protocol as an unspoofed message, wherein the second platform tears down, during a predetermined period, the unspoofed connection in response to the identified message to avoid delaying startup of a spoofed connection with the remote platform.

9. (Previously Amended) The system according to claim 8, wherein the second platform restarts the spoofed connection with another host.

10. (Original) The system according to claim 8, wherein the second platform has a timer to measure the predetermined period, the second platform being configured to determine whether the timer has expired and forwarding unspoofed messages to the remote platform.

11. (Original) The system according to claim 8, wherein the prescribed protocol is the Transmission Control Protocol, the second platform being configured to determine whether global TCP spoofing is enabled and to selectively forward TCP segments unspoofed to the remote platform.

12. (Original) The system according to claim 8, further comprising:
a backbone connection providing connectivity between the second platform and the remote platform, wherein the second platform configured to forward a spoofed message over the backbone connection.

13. (Original) The system according to claim 12, wherein the backbone connection is established over a satellite network.

14. (Original) The system according to claim 8, wherein the second platform is configured to forward messages associated with another protocol to the remote platform irrespective of the predetermined period.

15. (Previously Amended) A communication gateway for providing redundant communication in a communication system having a remote platform, the gateway comprising:
a communication interface configured to communicate with a primary gateway configured to support a spoofed connection over a backbone connection to the remote platform; and
a processor coupled to the communication interface and configured to restart a spoofed connection upon detection of a redundancy switch from a primary gateway,

wherein unspoofed messages are forwarded after a predetermined period to avoid delaying the restart of the spoofed connection.

16. (Previously Amended) The gateway according to claim 15, wherein the processor is configured to invoke a reset function to transmit a reset message to the host via the communication interface to tear down a connection transporting unspoofed messages.

17. (Canceled)

18. (Previously Presented) The gateway according to claim 15, wherein the processor is configured determine whether global Transmission Control Protocol (TCP) spoofing is enabled and to selectively forward TCP segments unspoofed to a remote platform.

19. (Canceled)

20. (Previously Presented) The gateway according to claim 15, wherein the backbone connection includes a space link over a satellite network.

21. (Canceled)

22. (Previously Amended) A communication gateway for providing redundant communication in a communication system, the gateway comprising:

means for detecting a redundancy switch condition;

means for identifying a message received over a connection according to a prescribed protocol as an unspoofed message;

means for tearing down, during a predetermined period, the connection based upon the identified message; and

means for restarting a spoofed connection upon detection of the redundancy switch condition, wherein the predetermined period is set to minimize delay for restarting of the spoofed connection.

23. (Previously Amended) The gateway according to claim 22, further comprising:

means for invoking a reset function, wherein the reset function transmits a reset message to a local host that forwarded the message to tear down the connection.

24. (Original) The gateway according to claim 22, further comprising:

means for determining whether the predetermined period has expired; and

means for forwarding unspoofed messages to a remote platform based upon the expiration of the predetermined period.

25. (Original) The gateway according to claim 22, wherein the prescribed protocol is the Transmission Control Protocol, the gateway further comprising:

means for determining whether global TCP spoofing is enabled; and

means for selectively forward TCP segments unspoofed to a remote platform.

26. (Previously Presented) The gateway according to claim 22, further comprising:

means for establishing a backbone connection to a remote platform; and

means for forwarding a spoofed message over the backbone connection to a remote host.

27. (Original) The gateway according to claim 26, wherein the backbone connection includes a space link over a satellite network.

28. (Original) The gateway according to claim 22, further comprising:
means for forwarding messages associated with another protocol to a remote platform
irrespective of the predetermined period.

29. (Previously Amended) A computer-readable medium carrying one or more sequences of one or more instructions for performing redundancy switching from a first platform to a second platform, the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

identifying a message received over an unspoofed connection according to a prescribed protocol as an unspoofed message;

tearing down, during a predetermined period, the unspoofed connection based upon the identifying step; and

restarting a spoofed connection between the second platform and a host, wherein the second platform serves as a redundant platform for the first platform, and the predetermined period is set to minimize delay for restarting of the spoofed connection.

30. (Previously Amended) The computer-readable medium according to claim 29, wherein the one or more processors further perform the step of:

invoking a reset function, wherein the reset function transmits a reset message to a local host that forwarded the message to tear down the unspoofed connection.

31. (Original) The computer-readable medium according to claim 29, wherein the one or more processors further perform the steps of:

determining whether the predetermined period has expired; and
forwarding unspoofed messages to a remote platform based upon the determining step.

32. (Original) The computer-readable medium according to claim 29, wherein the prescribed protocol is the Transmission Control Protocol, the one or more processors further performing the steps of:

determining whether global TCP spoofing is enabled; and
selectively forward TCP segments unspoofed to a remote platform.

33. (Original) The computer-readable medium according to claim 29, wherein the one or more processors further perform the steps of:

establishing a backbone connection from the second platform to a remote platform; and
forwarding a spoofed message over the backbone connection to a remote host.

34. (Original) The computer-readable medium according to claim 33, wherein the backbone connection in the establishing step includes a space link over a satellite network.

35. (Original) The computer-readable medium according to claim 29, wherein the one or more processors further perform the step of:

forwarding messages associated with another protocol to a remote platform irrespective of the predetermined period.

36. (New) The method according to claim 5, wherein the spoofed connection utilizes a protocol to alter behavior of the spoofed connection by performing one of three-way handshake spoofing, local data acknowledgement, connection to backbone connection multiplexing, data compression, or prioritization of connections.

37. (New) The system according to claim 12, wherein the spoofed connection utilizes a protocol to alter behavior of the spoofed connection by performing one of three-way handshake spoofing, local data acknowledgement, connection to backbone connection multiplexing, data compression, or prioritization of connections.

38. (New) The gateway according to claim 26, wherein the spoofed connection utilizes a protocol to alter behavior of the spoofed connection by performing one of three-way handshake spoofing, local data acknowledgement, connection to backbone connection multiplexing, data compression, or prioritization of connections.